Advisory Alert

Alert Number: AAA20260325 **Date:** March 25, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Remote Code Execution Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Use of Insufficiently Random Values Vulnerability
NetApp	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
Zabbix	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Node.js	**High, Medium, Low**	Multiple Vulnerabilities
F5	**High, Medium, Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-55182)
Description	NetApp has released a security update addressing a vulnerability that exists in their products. **CVE-2025-55182:** A pre-authentication remote code execution vulnerability exists in React Server Components. Multiple NetApp products incorporate React and are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetApp Data Classification NetApp Shift Toolkit
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20251205-0001

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the third party components of their product. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Storage Resource Manager – Versions prior to 6.0.0.2 Dell Storage Monitoring and Reporting – Versions prior to 6.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000443791/dsa-2026-111-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Use of Insufficiently Random Values Vulnerability (CVE-2025-7783)
Description	IBM has released a security update addressing a vulnerability that exists in their product. **CVE-2025-7783:** Use of Insufficiently Random Values vulnerability in form-data allows HTTP Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security QRadar Log Management AQL Plugin – Versions 1.0.0 - 1.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7267392

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-21441, CVE-2025-55184, CVE-2025-67779)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-21441:** urllib3 is a Python HTTP client library that supports efficient streaming of large responses. However, when handling HTTP redirects, it may unnecessarily read and decompress the entire response body—even before any data is requested—bypassing read limits. This can expose clients to decompression bomb attacks, where a malicious server triggers excessive resource consumption. **CVE-2025-55184:** A pre-authentication denial of service vulnerability exists in React Server Components. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints, which can cause an infinite loop that hangs the server process and may prevent future HTTP requests from being served. **CVE-2025-67779:** It was found that the fix addressing CVE-2025-55184 in React Server Components was incomplete and does not prevent a denial of service attack in a specific case, allowing unsafe deserialization of payloads from HTTP requests to Server Function endpoints. This can cause an infinite loop that hangs the server process and may prevent future HTTP requests from being served. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetApp Data Classification NetApp Shift Toolkit
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20260130-0010 • https://security.netapp.com/advisory/ntap-20251219-0014 • https://security.netapp.com/advisory/ntap-20251219-0015

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50697, CVE-2023-53781, CVE-2025-21738, CVE-2025-38159, CVE-2025-38488, CVE-2025-40258, CVE-2025-68284, CVE-2025-68285, CVE-2025-68813, CVE-2025-71085)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260992-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260997-1/

Affected Product	**Ubuntu**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerability (CVE-2025-40215, CVE-2025-21780, CVE-2024-56640, CVE-2024-49927, CVE-2022-49267, CVE-2022-49072, CVE-2022-48875, CVE-2021-47599)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu – Versions 18.04 and 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8098-4

Affected Product	**Zabbix**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerability (CVE-2026-23919, CVE-2026-23920, CVE-2026-23921, CVE-2026-23923, CVE-2026-23924)
Description	Zabbix has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Zabbix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Zabbix Server & Proxy Versions: • 6.0.0 – 6.0.40 • 7.0.0 – 7.0.21 • 7.2.0 – 7.2.14 • 7.4.0 – 7.4.5 Zabbix API Versions: • 7.0.0 – 7.0.21 • 7.2.0 – 7.2.14 • 7.4.0 – 7.4.5 Zabbix Frontend Versions: • 7.4.0 – 7.4.6 Zabbix Agent 2 Versions: • 6.0.0 – 6.0.43 • 7.0.0 – 7.0.22 • 7.4.0 – 7.4.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.zabbix.com/browse/ZBX-27638 • https://support.zabbix.com/browse/ZBX-27639 • https://support.zabbix.com/browse/ZBX-27640 • https://support.zabbix.com/browse/ZBX-27641 • https://support.zabbix.com/browse/ZBX-27642

Affected Product	**IBM**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerability (CVE-2025-14917, CVE-2025-14915, CVE-2026-1561, CVE-2026-29063, CVE-2023-2454, CVE-2023-5869, CVE-2024-7348, CVE-2024-10976, CVE-2022-41862, CVE-2023-2455, CVE-2024-10978, CVE-2023-5870, CVE-2023-5868, CVE-2022-2625, CVE-2024-10979, CVE-2024-0985, CVE-2023-39417, CVE-2024-10977, CVE-2026-0994)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Application Server – Liberty – Versions 17.0.0.3-26.0.0.3 IBM QRadar SIEM • Network Threat Analytics – Versions 1.4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7267345 • https://www.ibm.com/support/pages/node/7267362 • https://www.ibm.com/support/pages/node/7267347 • https://www.ibm.com/support/pages/node/7267351 • https://www.ibm.com/support/pages/node/7267391

Affected Product	**Node.js**
Severity	**High,** **Medium,** **Low**
Affected Vulnerability	Multiple Vulnerability (CVE-2026-21637, CVE-2026-21710, CVE-2026-21711, CVE-2026-21712, CVE-2026-21713, CVE-2026-21714, CVE-2026-21717, CVE-2026-21715, CVE-2026-21716)
Description	Node.js has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Node.js advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Node.js Versions: • 20.x • 22.x • 24.x • 25.x Dependencies: • undici (6.24.1, 7.24.4) on 22.x, 24.x, 25.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/march-2026-security-releases

Affected Product	**F5**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27654, CVE-2026-27651, CVE-2026-27784, CVE-2026-28753, CVE-2026-32647, CVE-2026-28755)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NGINX Plus • Versions R32 - R36 NGINX Open Source • Versions 1.0.0 - 1.29.6 • Versions 0.5.13 - 0.9.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000160382 • https://my.f5.com/manage/s/article/K000160383 • https://my.f5.com/manage/s/article/K000160364 • https://my.f5.com/manage/s/article/K000160367 • https://my.f5.com/manage/s/article/K000160366 • https://my.f5.com/manage/s/article/K000160368

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Muliple Vulnerabilities (CVE-2025-38024, CVE-2025-40240, CVE-2025-71085, CVE-2022-49985, CVE-2023-53539)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:5727 • https://access.redhat.com/errata/RHSA-2026:5693 • https://access.redhat.com/errata/RHSA-2026:5691 • https://access.redhat.com/errata/RHSA-2026:5689

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.